

EIGENVALUES OF SYMMETRIC MATRICES OVER INTEGRAL DOMAINS

MARIO KUMMER

ABSTRACT. Given an integral domain A we consider the set of all integral elements over A that can occur as an eigenvalue of a symmetric matrix over A . We give a sufficient criterion for being such an element. In the case where A is the ring of integers of an algebraic number field this sufficient criterion is also necessary and we show that the size of matrices grows linearly in the degree of the element. The latter result settles a questions raised by Bass, Estes and Guralnick.

1. INTRODUCTION

Let A be an integral domain with field of fractions $K = \text{Quot}(A)$. Let \bar{K} be the algebraic closure of K . We consider the question of which elements $\theta \in \bar{K}$ are an eigenvalue of a symmetric matrix over A . We denote this set by $\mathfrak{E}(A)$. Obviously, $\mathfrak{E}(A)$ is a subset of the integral closure \bar{A} of A in \bar{K} . It was shown in [BEG94] that $\mathfrak{E}(A)$ is in fact a subring of \bar{A} . Moreover, every $\theta \in \mathfrak{E}(A)$ must be *totally real over A* : For every ring homomorphism $A \rightarrow R$ to a real closed field, every prime ideal of $A[\theta] \otimes_A R$ must be a real prime ideal, i.e. with formally real residue field. We denote by A^{Re} the set of all totally real elements over A in \bar{A} . Estes [Est92] showed that $\mathfrak{E}(\mathbb{Z}) = \mathbb{Z}^{\text{Re}}$. Later Bass, Estes and Guralnick [BEG94] showed that $\mathfrak{E}(A) = A^{\text{Re}}$ in the case where A is a Dedekind domain or when -1 is a sum of squares in A .

Let A be any commutative ring with 1. If M is a symmetric matrix over A , then its characteristic polynomial has the property that its image under all homomorphisms from A to a real closed field R has all of its zeros in R . We call polynomials with this property *real zero polynomials*. If furthermore for every such homomorphism all zeros of its image are simple, we call it a *strict real zero polynomial*. We denote by $p(A)$ the *Pythagoras number* of A , i.e. the smallest number q such that every sum of squares in A is a sum of q squares in A . If no such number exists, let $p(A) = \infty$. Our main result is the following.

Theorem. *Let $f \in A[X]$ be a strict real zero polynomial of degree n . Then f divides the characteristic polynomial of a symmetric matrix $M \in \text{Sym}_r(A)$ with $r \leq (2p(A) + 1)n$.*

If A is an integral domain, this shows that every $\theta \in A^{\text{Re}}$ which is a zero of a strict real zero polynomial is the eigenvalue of a symmetric matrix over A . Furthermore, if A is the ring of integers of an algebraic number field, then the minimal polynomial of every $\theta \in A^{\text{Re}}$ is a strict real zero polynomial. Therefore, we get the following corollary.

Corollary. *Let A be the ring of integers of an algebraic number field. Every $\theta \in A^{\text{Re}}$ of degree n over A is an eigenvalue of a symmetric matrix over A of size at most $(2p(A) + 1)n$.*

2010 *Mathematics Subject Classification.* Primary: 11C20, 13J30.

The author was supported by the Studienstiftung des deutschen Volkes.

Note that if A is the ring of integers of an algebraic number field, then $p(A)$ is always finite [Sch80]. In the case of $A = \mathbb{Z}$ one has $p(\mathbb{Z}) = 4$ by Lagrange's Four-Square Theorem. Thus, the above result answers the following question raised by Bass, Estes and Guralnick to the affirmative with $c = 9$.

Question ([BEG94]). *Is there a constant c such that every $\theta \in \mathbb{Z}^{\text{Re}}$ is an eigenvalue of a symmetric integral matrix of size at most $c \cdot \deg_{\mathbb{Z}}(\theta)$?*

The main ideas used in this work were motivated by the theory of definite determinantal representations of hyperbolic polynomials in which similar questions are considered, however always over the ring of real polynomials. For a survey on this topic we refer to [Vin12].

2. PRELIMINARIES

Let A always be a commutative ring with 1. The set of sums of squares in A , i.e. elements of the form $a_1^2 + \dots + a_r^2$ with $a_i \in A$, is denoted by ΣA^2 . The set of matrices over A of size $m \times n$ is denoted by $\text{Mat}_{m,n}(A)$. The set of symmetric matrices over A of size n is denoted by $\text{Sym}_n(A)$. We will make use of the *real spectrum* of a ring. Given a ring A the real spectrum $\text{Sper } A$ is the set of all pairs $\alpha = (\mathfrak{p}, P)$ where \mathfrak{p} is a prime ideal of A and P is an ordering of the residue field $\kappa(\mathfrak{p})$. A prime ideal of A is a *real prime ideal* if the residue class field $\kappa(\mathfrak{p})$ has at least one ordering. A field that has at least one ordering is called *formally real*. A field K is formally real if and only if -1 is not a sum of squares in K if and only if there is a homomorphism $K \rightarrow R$ to a real closed field R . Let $\alpha = (\mathfrak{p}, P) \in \text{Sper } A$ and let $\rho_{A,\mathfrak{p}} : A \rightarrow \kappa(\mathfrak{p})$ be the canonical homomorphism. We denote by $\text{Supp}(\alpha) = \mathfrak{p}$ the support of α , i.e. the prime ideal corresponding to α . For any element $f \in A$ we say that $f(\alpha) \geq 0$, i.e. f is nonnegative in α , if $\rho_{A,\mathfrak{p}}(f) \in P$. We write $f(\alpha) > 0$, i.e. f is positive, if $f(\alpha) \geq 0$ and $f \notin \text{Supp}(\alpha)$. We say that $f \in A$ is nonnegative (positive) on $\text{Sper } A$ if it is nonnegative (positive) in every point of $\text{Sper } A$. We will need the following crucial result from real algebra cf. [KS89, III §9, Thm. 4]. It is also known as Stengle's Positivstellensatz.

Theorem 2.1 (Krivine's Positivstellensatz). *Let $a \in A$ be positive on $\text{Sper } A$. Then there are $s, t \in \Sigma A^2$ such that $(1 + s)a = 1 + t$.*

We refer to the book of Bochnak, Coste and Roy [BCR98] for proofs and more results on the real spectrum.

Definition 2.2. Let $\varphi : A \rightarrow B$ be a finite ring homomorphism. We say that φ is *totally real* if for every homomorphism $A \rightarrow R$ to a real closed field R every prime ideal of $B \otimes_A R$ is real. If A is an integral domain, we say that $\theta \in \bar{A}$ is *totally real over A* if $A \rightarrow A[\theta]$ is totally real. The set of all elements that are totally real over A in \bar{A} is denoted by A^{Re} .

Remark 2.3. Let K be a field and \bar{K} its algebraic closure. Let $\theta \in \bar{K}$ and $d = [K[\theta] : K]$. The field extension $K \subseteq K[\theta]$ is totally real if and only if every ordering of K has exactly d distinct extensions to $K[\theta]$. This is equivalent to θ lying in every real closed subfield of \bar{K} . Thus, K^{Re} is the intersection of all real closed fields in \bar{K} . If A is an integral domain, then it follows that A^{Re} is the set of all $\theta \in \bar{A}$ such that $\varphi(\theta) \in \text{Quot}(\varphi(A))^{\text{Re}}$ for every homomorphism from \bar{A} to an algebraically closed field. Thus, the above definition for A^{Re} coincides with the definition from [BEG94].

Definition 2.4. A monic polynomial $f \in A[X]$ is called a *real zero polynomial* if for all homomorphisms $A \rightarrow R$ to a real closed field R the image of f under the induced map $A[X] \rightarrow R[X]$ has all of its zeros in R . If moreover all of them are simple zeros (for all $A \rightarrow R$), then f is a *strict zero polynomial*.

Example 2.5. The characteristic polynomial of any $M \in \text{Sym}_n(A)$ is a real zero polynomial.

Remark 2.6. For any real zero polynomial $f \in A[X]$ the homomorphism

$$A \rightarrow A[X]/(f)$$

is totally real. Thus, roots of real zero polynomials over integral domains are totally real.

Example 2.7. If $\text{Sper } A = \emptyset$, then every monic polynomial $f \in A[X]$ is a strict real zero polynomial.

Example 2.8. Let R be a real closed field and $A = R[z_1, \dots, z_n]$. The polynomial $f = X^2 - (z_1^2 + \dots + z_n^2) \in A[X]$ is a real zero polynomial but not a strict real zero polynomial: Just consider the morphism $A \rightarrow R$ that sends every z_i to zero.

Definition 2.9. A symmetric matrix $M \in \text{Sym}_n(A)$ is *positive (semi-)definite* if for every homomorphism $\varphi : A \rightarrow R$ to a real closed field R the matrix $\varphi(A)$ is positive (semi-)definite.

Remark 2.10. Let $f \in A[X]$ be a monic polynomial and let $B = A[X]/(f)$. As an A -module B is free of rank $n = \deg f$. An A -basis is given by the residue classes of $1, X, \dots, X^{n-1}$. The *companion matrix* of f is the representing matrix C of the A -linear map $B \rightarrow B$, $h \mapsto \bar{X} \cdot h$ with respect to this basis. Its characteristic polynomial is f . Let $g \in A[X]$ be a polynomial of degree at most $n - 1$. Letting Y be a new variable one can write

$$\frac{f(Y) \cdot g(X) - f(X) \cdot g(Y)}{Y - X} = \sum_{1 \leq i, j \leq n} b_{i,j} Y^{i-1} X^{j-1}$$

where the $b_{i,j}$ are polynomial expressions in the coefficients of f and g . The *Bézout matrix* is the matrix $B(f, g) = (b_{i,j})_{1 \leq i, j \leq n}$. The determinant of the Bézout matrix is the resultant of f and g , i.e. $\det B(f, g) \in \mathfrak{p}$ for some prime ideal \mathfrak{p} of A if and only if the residue classes of f and g in $\kappa(\mathfrak{p})[X]$ have a common zero in the algebraic closure of $\kappa(\mathfrak{p})$. In particular, $B(f, 1)$ is invertible. Moreover, it is not hard to see that the Bézout matrix is symmetric and satisfies $B(f, g_1 + g_2) = B(f, g_1) + B(f, g_2)$ as well as $CB(f, g) = B(f, g)C^t$. The Bézout matrix $B(f, f')$ where f' is the derivative of f is positive semidefinite if and only if f is a real zero polynomial. It is positive definite if and only if f is a strict real zero polynomial. For proofs of these classical known results and more information we refer to [KN81, §2.2].

3. A POSITIVSTELLENSATZ

In this section we prove a Positivstellensatz for matrices over a ring A similar to Krivine's Positivstellensatz. Note that this is an ungraded version of the Positivstellensatz proved and used in [Kum13] that holds over the graded ring of real polynomials. The proof is also very similar.

Definition 3.1. A symmetric matrix $M \in \text{Sym}_n(A)$ is a *sum of squares* if there is a matrix $Q \in \text{Mat}_{m,n}(A)$ such that $M = Q^t Q$.

Remark 3.2. If $M \in \text{Sym}_n(A)$ is a sum of squares and $a \in A$, then $a^2 M$ is a sum of squares as well.

Remark 3.3. A symmetric matrix $M \in \text{Sym}_n(A)$ is a sum of squares if and only if there are (column) vectors $v_1, \dots, v_m \in A^n$ such that

$$M = v_1 v_1^t + \dots + v_m v_m^t.$$

Thus the sum of matrices that are a sum of squares is again a sum of squares.

Remark 3.4. A matrix that is a sum of squares is positive semidefinite.

Lemma 3.5. *Let $M \in \text{Sym}_n(A)$ be positive definite. Then there are $s \in \Sigma A^2$ and $Q \in \text{Mat}_{m,n}(A)$ such that $(1+s)M = Q^t Q$ and $m \leq np(A)$.*

Proof. The statement is trivial if $\text{Sper } A = \emptyset$. In that case -1 is a sum of squares in A , thus we can take $s = -1$ and $Q = 0$. Therefore, we can assume that $\text{Sper } A \neq \emptyset$.

Let $S \subseteq A$ be the multiplicative subset of all elements of A that are positive on $\text{Sper } A$. In A_S we can diagonalize the quadratic form represented by M using the Gram–Schmidt process: Because M is positive definite, we only have to divide by elements that are positive on $\text{Sper } A$. Thus we have a $n \times n$ matrix Q_0 and a diagonal matrix D_0 with entries in A_S such that $M = Q_0^t D_0 Q_0$ holds in A_S . Clearing denominators gives an $s_1 \in S$, a matrix Q_1 and a diagonal matrix D_1 , both with entries in A , such that $s_1 M = Q_1^t D_1 Q_1$. Note that the diagonal entries of D_1 are in S . Thus by Krivine’s Positivstellensatz there is a sum of squares $s_2 \in \Sigma A^2$ such that s_2 multiplied with s_1 and with any entry of D_1 is in $1 + \Sigma A^2$. Every diagonal entry of $s_2 D_1$ is a sum of at most $p(A)$ squares. This gives the claim. \square

Definition 3.6. For $M \in \text{Sym}_n(A)$ we denote by $\Sigma(M)$ the subset of A^n consisting of all elements $v \in A^n$ such that

$$sM = v^t v + N$$

for some $s \in \Sigma A^2$ and $N \in \text{Sym}_n(A)$ that are both a sum of squares.

Lemma 3.7. *The subset $\Sigma(M)$ is a submodule of A^n .*

Proof. It is clear that $A \cdot \Sigma(M) \subseteq \Sigma(M)$. The following identity shows that $\Sigma(M) + \Sigma(M) \subseteq \Sigma(M)$:

$$(v_1 + v_2)^t(v_1 + v_2) + (v_1 - v_2)^t(v_1 - v_2) = 2 \cdot (v_1^t v_1 + v_2^t v_2). \quad \square$$

Example 3.8. Let $a \in A$ be positive on $\text{Sper } A$. Then $\Sigma(a) = A$ by Krivine’s Positivstellensatz.

Lemma 3.9. *Let $M \in \text{Sym}_n(A)$, $a \in A$, $v \in A^n$ and $b \in \Sigma(a)$. If $av \in \Sigma(M)$, then $b^2 v \in \Sigma(M)$.*

Proof. There are $s_1, r \in \Sigma A^2$ such that $s_1 a = b^2 + r$. If $av \in \Sigma(M)$, then there are $s_2 \in \Sigma A^2$ and a sum of squares $N \in \text{Sym}_n(A)$ such that $s_2 M = a^2 v^t v + N$. Multiplying the second equation by s_1^2 and applying the first equation gives us

$$\begin{aligned} s_1^2 s_2 M &= (b^2 + r)^2 v^t v + s_1^2 N \\ &= (b^2 v)^t (b^2 v) + (2b^2 r + r^2) v^t v + s_1^2 N. \end{aligned}$$

Thus $b^2 v \in \Sigma(M)$. \square

Corollary 3.10. *Let $M \in \text{Sym}_n(A)$ and $a \in (\Sigma(M) : A^n)$. Then $b^2 \in (\Sigma(M) : A^n)$ for all $b \in \Sigma(a)$.*

Proof. For all $v \in A^n$ we have $av \in \Sigma(M)$ and thus $b^2 v \in \Sigma(M)$ for all $b \in \Sigma(a)$ by Lemma 3.9. \square

Lemma 3.11. *Let $M \in \text{Sym}_n(A)$ be positive definite. The ideal $I = (\Sigma(M) : A^n)$ is not contained in any real prime ideal.*

Proof. By Lemma 3.5 there are $s \in \Sigma A^2$ and $Q \in \text{Mat}_{m,n}(A)$ such that $(1+s)M = Q^t Q$. We can assume that $m \geq n$. Let $J \subseteq \{1, \dots, m\}$ be a subset with exactly n

elements. Let Q_J be the submatrix of Q with the rows from J and $q_J = \det(Q_J)$ its determinant. By the Theorem of Cauchy–Binet we have that

$$\det((1+s)M) = \det(Q^t Q) = \sum_{J \subseteq \{1, \dots, m\}, |J|=n} q_J^2.$$

Since $(1+s)M$ is positive definite, its determinant is positive on $\text{Sper } A$. This means that the ideal generated by the q_J 's is not contained in a real prime ideal. Thus it remains to show that $q_J \in I$ for every subset $J \subseteq \{1, \dots, m\}$ with n elements. We consider the identity $Q_J^t \text{adj}(Q_J)^t = q_J I_n$ where $\text{adj}(Q_J)$ is the adjugate matrix of Q_J . Now for any $v \in A^n$ we get by multiplying v from the right to this identity that $q_J v$ is an A -linear combination of the rows of Q which are in $\Sigma(M)$. This implies the claim. \square

Lemma 3.12. *Let $I \subseteq A$ be an ideal that is not contained in any real prime ideal of A . There is a $f \in I$ with $\Sigma(f) = A$.*

Proof. Let $B = A/I$. Then -1 is positive on $\text{Sper } B = \emptyset$, thus $-1 \in \Sigma B^2$ by Krivine's Positivstellensatz. Therefore, $1+s \in I$ for some $s \in \Sigma A^2$ and clearly $\Sigma(1+s) = A$. \square

Corollary 3.13. *If $M \in \text{Sym}_n(A)$ is positive definite, then $(\Sigma(M) : A^n) = A$ and thus $\Sigma(M) = A^n$.*

Proof. By Lemma 3.11 the ideal $I = (\Sigma(M) : A^n)$ is not contained in a real prime ideal. Thus by Lemma 3.12 there is a $f \in I$ with $1 \in \Sigma(f)$. Thus by Corollary 3.10 we have $1 \in (\Sigma(M) : A^n)$, i.e. $(\Sigma(M) : A^n) = A$. \square

Theorem 3.14. *For every positive definite $M \in \text{Sym}_n(A)$ there are $s \in \Sigma A^2$ and $Q \in \text{Mat}_{m,n}(A)$ such that $sM = I_n + Q^t Q$ and $m \leq 2np(A)$.*

Proof. There are $r \in \Sigma A^2$ and a sum of squares $N \in \text{Sym}_n(A)$ such that $rM = I_n + N$ by the preceding corollary. By Lemma 3.5 there are $r' \in \Sigma A^2$ and $Q' \in \text{Mat}_{m',n}(A)$ such that $(1+r')N = Q'^t Q'$ and $m' \leq np(A)$. Thus $r(1+r')M = I_n + r' I_n + Q'^t Q'$. Since r' is a sum of at most $p(A)$ squares, $r' I_n + Q'^t Q'$ is a sum of at most $2np(A)$ squares. \square

Remark 3.15. Like Lemma 3.5 the statement of Theorem 3.14 becomes trivial if $\text{Sper } A$ is empty because in that case $-I_n$ is a sum of squares.

4. STRICT REAL ZERO POLYNOMIALS

Theorem 4.1. *Let $f \in A[X]$ be a strict real zero polynomial of degree n . Then f divides the characteristic polynomial of a symmetric matrix $M \in \text{Sym}_r(A)$ with $r \leq (2p(A) + 1)n$.*

Proof. Let C be the companion matrix of f and let $B = B(f, f')$ which is positive definite. By Theorem 3.14 there are $s \in \Sigma A^2$ and $Q \in \text{Mat}_{m,n}(A)$ such that $sB = I + Q^t Q$ and $m \leq 2np(A)$. Consider the matrices

$$Q' = \begin{pmatrix} I_n & Q^t \\ 0 & I_m \end{pmatrix} \text{ and } M' = \begin{pmatrix} C & 0 \\ Q C^t & -Q C^t Q^t \end{pmatrix}.$$

The characteristic polynomial of M' is divisible by f and Q' is invertible over A . Thus the characteristic polynomial of $M = Q'^{-1} M' Q'$ is also divisible by f . It is

$$M = \begin{pmatrix} C - Q^t Q C^t & C Q^t \\ Q C^t & 0 \end{pmatrix}$$

and it follows from $BC^t = CB$ that this matrix is symmetric. The size of M is $m + n \leq (2p(A) + 1)n$. \square

Remark 4.2. The statement of Theorem 4.1 is in general not true if we only assume f to be a real zero polynomial. In [BEG94, Ex. 1.5] they give an example of a noetherian factorial domain A and an element $a \in A$ such that $f = X^2 - a$ is a real zero polynomial that does not divide the characteristic polynomial of any symmetric matrix over A .

Corollary 4.3. *Let A be an integral domain and let $\theta \in A^{\text{Re}}$ be a root of a strict real zero polynomial of degree n . Then θ is an eigenvalue of a suitable $M \in \text{Sym}_r(A)$ with $r \leq (2p(A) + 1)n$.*

As a byproduct we get that every integral element over a ring with empty real spectrum is an eigenvalue of a suitable symmetric matrix over this ring. This has already been shown in [BEG94, Thm. 3.8].

Corollary 4.4. *If $\text{Sper } A = \emptyset$, then every element $\theta \in \bar{A}$ is an eigenvalue of a suitable $M \in \text{Sym}_r(A)$.*

Corollary 4.5. *Let A be an integral domain with field of fractions K . Assume that no non-zero prime ideal of A is real and let $f \in A[X]$ be a real zero polynomial of degree n . Then f divides the characteristic polynomial of a symmetric matrix $M \in \text{Sym}_r(A)$ with $r \leq (2p(A) + 1)n$.*

Proof. The assumption on A implies that every real zero polynomial that is irreducible over K is a strict real zero polynomial. If f is reducible, we can take the direct sum of the matrices that we get for each irreducible factor. \square

Corollary 4.6. *Let A be the ring of integers of an algebraic number field. Every $\theta \in A^{\text{Re}}$ of degree n is an eigenvalue of a suitable $M \in \text{Sym}_r(A)$ with $r \leq (2p(A) + 1)n$.*

Proof. Apply the preceding corollary to the minimal polynomial of θ . \square

Remark 4.7. The Pythagoras number of the ring of integers A of an algebraic number field is always finite [Sch80]. Thus, for every such A there is a positive integer c such that every $\theta \in A^{\text{Re}}$ is an eigenvalue of a symmetric matrix over A of size at most $c \cdot \deg_A(\theta)$. One reason why we are not able to proof such a bound for arbitrary Dedekind domains is because in general they do not have finite Pythagoras number (even if their field of fractions has finite Pythagoras number, see [CDLR82, §4]). Another reason is that in general not every real zero polynomial is a strict real zero polynomial.

Acknowledgements. I would like to thank Christoph Hanselka for drawing my attention to this problem and for helpful discussions and remarks, especially on the proof of Lemma 3.5. I also thank the Studienstiftung des deutschen Volkes for their financial and ideal support.

REFERENCES

- [BCR98] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.
- [BEG94] Hyman Bass, Dennis R. Estes, and Robert M. Guralnick. Eigenvalues of symmetric matrices and graphs. *J. Algebra*, 168(2):536–567, 1994.
- [CDLR82] M. D. Choi, Z. D. Dai, T. Y. Lam, and B. Reznick. The Pythagoras number of some affine algebras and local algebras. *J. Reine Angew. Math.*, 336:45–82, 1982.
- [Est92] Dennis R. Estes. Eigenvalues of symmetric integer matrices. *J. Number Theory*, 42(3):292–296, 1992.

- [KN81] M. G. Kreĭn and M. A. Naĭmark. The method of symmetric and Hermitian forms in the theory of the separation of the roots of algebraic equations. *Linear and Multilinear Algebra*, 10(4):265–308, 1981. Translated from the Russian by O. Boshko and J. L. Howland.
- [KS89] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*, volume 63 of *Vieweg Studium: Aufbaukurs Mathematik [Vieweg Studies: Mathematics Course]*. Friedr. Vieweg & Sohn, Braunschweig, 1989.
- [Kum13] Mario Kummer. Determinantal representations and Bézoutians. *arXiv*, 1308.5560, 2013.
- [Sch80] Rudolf Scharlau. On the Pythagoras number of orders in totally real number fields. *J. Reine Angew. Math.*, 316:208–210, 1980.
- [Vin12] Victor Vinnikov. LMI representations of convex semialgebraic sets and determinantal representations of algebraic hypersurfaces: past, present, and future. In *Mathematical methods in systems, optimization, and control*, volume 222 of *Oper. Theory Adv. Appl.*, pages 325–349. Birkhäuser/Springer Basel AG, Basel, 2012.

UNIVERSITÄT KONSTANZ, GERMANY

E-mail address: Mario.Kummer@uni-konstanz.de